IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	**CRIMINAL NO. ELH-19-0450**
STEPHEN WAYNE CORMACK,	:	
	:	
Defendant.	:	

...ooOoo...

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS TANGIBLE AND DERIVATIVE EVIDENCE

Now comes the United States of America by its attorneys, Jonathan F. Lenzner, Acting United States Attorney for the District of Maryland, and Matthew J. Maddox, Assistant United States Attorney, and responds in opposition to the Defendant Stephen Wayne Cormack's Motion to Suppress Tangible and Derivative Evidence (the "Motion to Suppress").

I. BACKGROUND

A. Defendant's Employment with the State of Maryland

Defendant Cormack was hired as an administrative officer by the Maryland Department of General Services ("DGS") in 1999. DGS is a department of the Maryland State government.

On August 28, 2000, the Defendant signed a document acknowledging his receipt of the DGS Employee Handbook. *See* Exhibit 1 (Acknowledgement Receipt). The Employee Handbook included various DGS directives, including a directive titled "Acceptable Use Statement for Computing Resources." *See* Exhibit 2 (Excerpt of DGS Employee Handbook).

The Acceptable Use Statement "outlines acceptable use of the computing systems and equipment owned and operated by the Maryland Department of General Services (DGS)." *Id.* at

4. The purpose of the document "is to ensure that all DGS users (support personnel and management) use the DGS computing systems and facilities in a effective, efficient, ethical and lawful manner." *Id.* A statement of policy within the document provides that "DGS computing resources are to be used only for the purpose for which they are authorized and are not to be used for non-DGS related activities[,]" and that "[t]he DGS Information Technologies Group may monitor network traffic, e-mail transmissions, and internet activity." *Id.* at 4. Several specific provisions are included in the policy statement, including the following: "8. Electronic communication facilities (such as Email or Internet) are for authorized government use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from or stored on DGS systems." *Id.* at 5. The Acceptable Use Statement provides further that

> Any noncompliance with these requirements will constitute a security violation and will be reported to the Secretary of DGS and will result in short-term or permanent loss of access to DGS computing resources. Individuals found to have violated this policy may receive a: written reprimand; forfeiture of annual leave; demotion; suspension; denial of annual pay increase; or termination. Serious violations may result in civil or criminal prosecution.

In signing the Acknowledgment Receipt, the Defendant affirmed that he understood that the Employee Handbook "is an employee reference source of information concerning State policies, procedures, benefits and rules, but does not represent all administrative directives, benefits, policies, procedures and rules currently in effect." Exhibit 1. The Defendant further affirmed his understanding that "the State and the Department of General Services has the right from time to time to change existing administrative directives, benefits, policies, procedures and/or rules and to formulate and put into effect additional directives, benefits, policies, procedures and/or rules." *Id.*

On or about August 4, 2016, DGS Office of the Secretary circulated a memorandum to all existing DGS employees titled "DGS Policy – Inappropriate Use of eMail and Internet." *See* Exhibit 3 (DGS Inappropriate Use Policy Memorandum). The memorandum states, in part, the following:

> Electronic communications are to be used only for authorized government business.
>
> Please be advised that the Department has a zero tolerance policy for the inappropriate use of State email and internet resources. . . . Fraudulent, harassing or obscene messages and/or materials shall not be created with, sent from, to, or stored on DGS systems. Access sexually explicit and/or gambling websites is also a violation of the Department's eMail and Internet policy.

According to personnel records provided to the Government, the Defendant's work responsibilities in 2019 included:

> To develop, implement and manage a plan to catalog, track and maintain the Division's archive of project drawings and specification documents in a manner that permits information to be retrieved in a timely manner.
>
> Establish a digital project document storage and retrieval process that is widely available to DGS employees across the state. Continually improve and update the digital documents as well as the storage and retrieval process by advising and proposing alternate methods of digitizing and electronically storing the Division's drawings and project specifications.
> . . .
>
> Maintain an adequate supply of office materials, track loaned office equipment and record the Division's credit card purchases. Assist with the development, execution and tracking of the annual budget for expendable office supplies, office machine maintenance contracts, and new equipment requirements.

In order for Defendant Cormack to complete his work duties, the State of Maryland provided him a workspace within a room at 301 West Preston Street, 14th Floor, Baltimore, Maryland ("Office C"). *See* Exhibit 4 (video stills of Office C). A sign posted outside the door to Office C listed the Defendant's name. The Defendant worked at a desk with a workstation in Office C that included a computer and related equipment provided by the State of Maryland. Office C also housed office supplies for use by DGS employees on the 14th floor as well as large filing cabinets for architectural blueprints the Defendant was charged with managing. During work hours, the Defendant left the door to Office C open, and the room was frequently and freely accessed by other employees to obtain office supplies or to access blueprints. The door was locked when the Defendant was not present, but another employee had a key and could open Office C for any employee who required access for work-related purposes.

The Defendant's work responsibilities entailed the regular and frequent use of his work computer and related equipment. A series of warning banners displayed to the Defendant whenever turning on and logging into his work computer. *See* Exhibit 5 (images of warning banners). One warning banner states as follows (emphasis added):

> This computing system is owned and operated by the State of Maryland, Department of Information Technology, and is for official use only by authorized personnel. Access and use of this system are subject to policies and rules. Unauthorized access, unauthorized attempted access, or unauthorized use of any State computing system is a violation of Section 7-302 of the Maryland Penal Code and/or applicable federal law, and may be subject to prosecution.
>
> Any and all users of this system and all the files on this system may be monitored, recorded, copied, inspected and disclosed to authorized personnel. **Therefore, users should have no reasonable expectation of privacy in the use of these resources. Anyone**

> **using this system expressly consents to such monitoring, recording, copying, inspecting, and disclosure at the discretion of authorized personnel.**

A separate warning banner states the following:

> *****WARNING*****WARNING*****WARNING*****
>
> Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of the system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose.
>
> In order to proceed past this display and continue the log-in process, the Defendant was required to click an "OK" button under the warning banner.

B. <u>Investigation of Defendant's Activity Involving Child Pornography</u>

In January 2019, another employee of DGS ("Witness 1") reported to a supervisor apparent misconduct by Defendant Cormack involving the use of his work computer. Witness 1 reported that, while in Office C, and while the Defendant was sitting at his work computer, Witness 1 observed the Defendant viewing an image of a child that Witness 1 believed to be child pornography. The supervisor reported the matter to Human Resources ("HR"), and HR reported the matter to Maryland Capitol Police, the security component of DGS.

On February 5, 2019, Witness 1 was interviewed by officers of Maryland Capital Police and Maryland State Police ("MSP") – Maryland Internet Crimes Against Children Task Force. During the interview, Witness 1 stated, in part, the following:

- Witness 1 went into Defendant Cormack's workspace and saw an image of what he believed to be child pornography on the Defendant's State computer. The image

depicted a male child of approximately 8 years of age posing in white underwear who appeared to be terrified. Witness 1 was certain that the intended purpose of the image was for sexual gratification. The Defendant immediately minimized the image file when Witness 1 walked into the room.

- A similar incident occurred several years prior when Witness 1 observed the Defendant viewing a suspicious website on his personal computer and observed the title "young Japanese boys" on the site. Witness 1 regretted not reporting the prior incident but that he had considered it a fluke. Witness 1 noticed several "red flag" instances over the years, and the Defendant's behavior had continued without stopping.

- Defendant Cormack was charged for several sexual offenses in approximately 1995.

- Defendant Cormack was "very into computers," tended to migrate from his work computer to his personal computer during the work day, and had a back-up drive that went home with him every night. The Defendant kept his personal laptop computer in the back of Office C near the supplies closet and, whenever someone approached, the Defendant closed the display. The Defendant always took his personal laptop with him to and from work.

- It pained Witness 1 to report Defendant Cormack. Witness 1 was certain of what he saw and felt that an investigation was warranted.

Witness 1 provided a hand-drawn map of Office C that depicted the location of Defendant Cormack's work and personal computer.

Following the interview of Witness 1, TFC Frank Donald of MSP obtained records of a prior investigation of the Defendant by Baltimore County Police Department, which revealed evidence that the Defendant had sexually abused several male minors while employed as a counselor at a recreation center in Parkville, Maryland. The Defendant was convicted of second-degree sexual assault in 1996.

In February 2019, the Chief Information Security Officer for the Maryland Department of Information Technology ("DoIT") remotely investigated the Defendant's use of the computer network at DGS and found that he could not obtain the Defendant's Internet search history.

After work hours on March 28, 2019, the Chief Information Security Officer, TFC Donald, and members of Maryland Capital Police and MSP Digital Forensics Lab entered Office C in order to investigate the Defendant's work computer. The Chief Information Security Officer authorized MSP to conduct a search of Office C and to seize evidence from the room, and signed a consent form reflecting this authorization. *See* Exhibit 6 (Consent to Search and Seize).

During a forensic preview of information stored on a State-issued external hard drive at the workstation, investigators observed an image of a male minor (estimated to be 14 or 15 years old) masturbating his erect penis. The image was located in the recycle bin of the external hard drive. The investigators imaged the external hard drive, cloned the internal hard drive in the Defendant's work computer, replaced these items at the workstation, and left Office C with the hard drives.

During subsequent review of the hard drives, MSP located evidence on the work computer reflecting the Defendant's interest in and efforts to view images of children for sexual gratification, including the following:

- Internet searches for "child porn" on 12 separate occasions using the work computer on March 8, 2018;
- Searches on video streaming website Youtube.com for "boys skinny dipping" using the work computer on September 9, 2018;
- Image files of scantily clothed and shirtless prepubescent boys stored in the "My Documents" folder on the work computer;
- Internet browser history reflecting informational materials about child sex abuse material and child pornography.

The forensic examination also revealed that data stored in the Defendant's work computer referenced frequent connection to an additional external hard drive. Investigators noted that the Defendant's work computer had cables attached to it that would allow him to easily attach an

external hard drive, but no external hard drives were attached to these cables during the covert investigation on March 28, 2019.

MSP subsequently obtained state warrants to search and seize evidence from Office C and the Defendant's residence at 24 Lyndale Avenue, Nottingham, Maryland. *See* Exhibit 7 (Search Warrant for Office C) and Exhibit 8 (Search Warrant for Residence). The search warrants were executed on May 2, 2019. The Defendant was present at his residence on that date, was advised of Miranda rights, signed a waiver, and voluntarily agreed to be interviewed by law enforcement. The Defendant stated, in part, the following:

- The briefcase Defendant Cormack ordinarily takes to work with him was located in his car, which was parked in front of his house. The briefcase contained two external hard drives, and one of the hard drives contained a back-up of the files in which the Defendant archives for work. Defendant Cormack backs up the files out of caution since files contained on the office network server have been lost in the past. The other hard drive contains photos of family and vacations and personal documents. There was no "pornography" on this hard drive.

- The Defendant did not use his work computer to view child pornography but he had used Google and, if child pornography came up, he would look at it.

- Defendant Cormack had a personal laptop computer at work that should be located in his office, either on the desk or in a grey cabinet. It was an Acer laptop computer, and he usually does not bring it home. The Defendant has the personal laptop at his work site because he has a color printer he uses to print out pictures of family and vacations to display in his office.

- Defendant Cormack did not produce, distribute, or save any child pornography, but he had looked at child pornography. The Defendant went on "Google at work" to look at child pornography and did not remember any search terms or used any specific "sites."

At Office C, pursuant to the search warrant, law enforcement seized two laptop computers (including a Acer laptop), several SD cards, two digital cameras, and other storage media.

Electronic storage media was also seized pursuant to the search warrant for the Defendant's residence.

Homeland Security Investigations ("HSI") obtained a federal search warrant to examine several items seized during the searches, including the Acer laptop computer and SD cards seized from Office C. *See* Exhibit 9 (Search Warrant for Devices). Forensic examination of the Acer laptop computer, its internal hard drive, and a SanDisk SD card revealed approximately 3,800 images and over 300 videos of child sexual abuse. Child pornography was also found on other electronic storage devices seized from the Defendant on May 2, 2019.\

C. Procedural Background

On September 19, 2019, a federal grand jury sitting in Baltimore, Maryland returned an Indictment charging the Defendant with Possession of Child Pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2256.

On February 26, 2021, the Defendant, through counsel, filed the Motion to Suppress, challenging the entry to Office C on March 28, 2019; the seizure of computer equipment from Office C on that date; the searches of the Defendant's residence and Office C on May 2, 2019; and the subsequent forensic examination of devices seized from those locations.

The Court should deny the Motion to Suppress because (1) the entry into Office C and examination of the Defendant's State-issued work computer equipment on March 28, 2019, was not a Fourth Amendment search; (2) even if these investigative measures constituted a search under the Fourth Amendment, the search was justified by consent of the Defendant and his employer, was reasonable in its inception and scope, and therefore reasonable under the Fourth Amendment; and (3) the searches of the Defendant's residence and Office C on May 2, 2019, and

subsequent forensic examination of devices seized from those locations were authorized by search warrants supported by probable cause.

II. ARGUMENT

A. The Entry into Office C and Investigation of the Work Computer on March 28, 2019, Was Not a Fourth Amendment Search.

The Defendant's Fourth Amendment rights were not implicated by investigators' entry into Office C on March 28, 2019, and investigation of his State-issued work computer equipment because the Defendant cannot show a legitimate expectation of privacy in these work facilities.

"The Fourth Amendment prohibits 'unreasonable searches and seizures' by government agents, including government employers or supervisors." *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (quoting U.S. Const. amend. IV). However, the protections of the Fourth Amendment only apply when government actors conduct a search or seizure where there is a constitutionally protected expectation of privacy. *United States v. Davis*, 690 F.3d 226, 241 (4th Cir. 2012) (citing *New York v. Class*, 475 U.S. 106, 112 (1986)). "When there is no reasonable expectation of privacy, the Fourth Amendment is not implicated." *Id.*

In order to demonstrate a legitimate expectation of privacy, a criminal defendant must show that he has an actual expectation of privacy, and that subjective expectation of privacy must be objectively reasonable. *United States v. Castellanos*, 716 F.3d 828, 832 (4th Cir. 2013) (citations omitted). "[I]n other words, it must be an expectation that society is willing to recognize as reasonable[.]" *Id.* (internal quotation marks and citation omitted); *see also Simons*, 206 F.3d at 398. The defendant bears the burden of showing a legitimate expectation of privacy in the

location searched or the item seized. *Castellanos*, 716 F.3d at 832 (citing *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)); *Simons*, 206 F.3d at 398 (citing cases).

"Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets[,]" but "office practices, procedures, or regulations may reduce legitimate privacy expectations." *Id.* (citations omitted). And, as a general matter, "the privacy interests of government employees in their place of work . . . , while not insubstantial, are far less than those found at home or in some other contexts" when "[b]alanced against the substantial government interests in the efficient and proper operation of the workplace[.]" *O'Connor v. Ortega*, 480 U.S. 709, 725 (1987). "Government offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may avoid exposing personal belongings at work by simply leaving them at home." *Id.*

A government employee's expectation of privacy in his or her workspace must be assessed in context. *Id.* at 717. "Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* Indeed, "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable." *Id.* at 718. Additionally, "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010).

In the context of the instant case, Defendant Cormack lacked any legitimate expectation of privacy in Office C and in the digital contents of his State-issued work computer and external hard

drive. It is important to note that Defendant Cormack cannot credibly claim that any actual expectation of privacy that was violated on March 28, 2019. Office C contained Defendant Cormack's workspace, but it was essentially a storage room that was regularly accessed by various other DGS employees. Although the Defendant had administrative oversight of items stored in Office C, these office supplies and other materials were for the general work-related use of his co-workers, and the space was made freely available to them. Thus, any expectation of privacy in Office C was undermined by the frequent traffic in and out of that room by various employees seeking office supplies and other materials.

Multiple district judges of this Court have held that there is no reasonable expectation of privacy in such an open office or common area of the workplace. *See Marrs v. Marriott Corp.*, 830 F. Supp. 274, 283 (D. Md. 1992) (Nickerson, J.) (no reasonable expectation of privacy in an open office); *Woodbury v. Victory Van Lines*, 286 F. Supp. 3d 685, 697 (D. Md. 2017) (Chuang, J.) ("Ordinarily, an employee does not have a reasonable expectation of privacy in the workplace."); *cf. O'Connor*, 480 U.S. at 718 ("[S]ome government offices may be so open to fellow employees . . . that no expectation of privacy is reasonable.").

Once inside Office C, Defendant Cormack's State-owned computer workstation was in plain view and, in any case, was not the Defendant's personal property, but rather the property of his employer, the State of Maryland. *See United States v. Bellina*, 665 F.2d 1335, 1341 (4th Cir. 1981) ("[O]ne has no legitimate expectation of privacy in any object whether it be in the home or a car or a plane if that object is exposed to plain view."); *United States v. Taylor*, 90 F.3d 903, 909 (4th Cir. 1996) (no reasonable expectation of privacy in objects exposed to plain view where viewer's presence at the vantage point is lawful).

Any claim by Defendant Cormack that he expected privacy in the use and contents of his State-issued work computer is neither credible nor reasonable. Any expectation of privacy in the use and contents of Defendant Cormack's work computer was eliminated by DGS's Internet use policy and multiple warning banners presented during the computer log-in process. *See United States v. Linder*, No. 12 CR 22-1, 2012 WL 3264924, at *8 (N.D. Ill. Aug. 9, 2012) (defendant "cannot credibly claim that he subjectively believed that his use of his government-issued data devices was private" after having received clear warnings "on multiple occasions that he had no legitimate expectation of privacy when he accessed the government's computer information system"). These warning banners provided regular notice that all computer use at DGS was restricted to official purposes by policy, was monitored, and could be disclosed. The Defendant was aware of the DGS policy and the State's right to monitor, inspect, and disclose computer activity, having signed an acknowledgment of receiving the policy (*see* Exhibit 1, Acknowledgement Receipt), having been re-notified of the policy in 2016 (*see* Exhibit 3, DGS Memorandum), and having received daily log-in warnings about the policy (*see* Exhibit 5, Warning Banners). Defendant could not have reasonably expected that the files on his State work computer would remain private.

Courts, including the Fourth Circuit and district judges of this Court, have held that employers' policies, including government employers, that put employees on notice that computer use is monitored negate any legitimate expectation of privacy. *See Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (government employee "did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use" in light of the agency policy that Internet use would be monitored and "placed employees on notice that they could not reasonably expect that

their Internet activity would be private"); *Sorensen v. Westec InterActive Sec., Inc.*, Civ. No. DKC-07-2841, 2008 WL 11367535, at *10 (D. Md. Sept. 2, 2008) (Chasanow, J.) (no reasonable expectation of privacy in work computer, Internet use, and email where employer policy states that employee computer usage is subject to monitoring, "[e]ven assuming that [employee] never received or read" employee handbook); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (notice of employer policy "that it could inspect the laptops that it furnished for the use of its employees . . . destroyed any reasonable expectation of privacy"); *Linder*, 2012 WL 3264924, at *7 ("Government employees do not maintain a reasonable expectation of privacy in the information stored on their computers when the employee is notified that their employer has retained the right to access or inspect the information stored there.").

This Court, the Fourth Circuit, and other courts also have held that the display of warning banners on computer systems, like those displayed on the Defendant's work computer in this case, eliminates any reasonable expectation of privacy in the use of the computer system. *See United States v. Hamilton*, 701 F.3d 404 (4th Cir. 2012) (emails not subject to marital privilege where computer policy expressly provides that users have "no expectation of privacy in their use of the Computer System" and all information stored in Computer System is "subject to inspection and monitoring at any time[,]" and user "had to acknowledge the policy by pressing a key to proceed to the next step of the log-on process, every time he logged onto his work computer"); *United States v. Bode*, Crim. No. ELH-12-158, 2013 WL 4501303, at *19–*20 (D. Md. Aug. 21, 2013) (Hollander, J.) (no reasonable expectation of privacy in private chat messages exchanged through website where warning banners notified user that messages were logged and supervised and could be disclosed to authorities); *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002) (no warrant

needed to examine of work computer seized from office of university professor when a splash screen provided notice depriving users of university computers of any legitimate expectation of privacy; *United States v. Bailey*, 272 F. Supp. 2d 822, 824 (D. Neb. 2003) (defendant "had no expectation of privacy in the work computer owned by someone else because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer"); *Linder*, 2012 WL 3264924, at *7 ("Courts have similarly held that banners and policies generally eliminate a reasonable expectation of privacy in the contents stored in a government users' network account.") (citing cases); *Aikens v. Ingram*, 71 F. Supp. 3d 562, 568–69 (E.D.N.C. 2014) (where log-on screens on computer system provided notice that email would be monitored, it would be unreasonable to expect email to remain private); *United States v. Wilson*, No. 3:15-CR-02838-GPC, 2017 WL 2733879, at *7 (S.D. Cal. June 26, 2017) ("This express monitoring policy regarding illegal content, which Defendant agreed to, rendered Defendant's subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable.").

1. *United States v. Simons*

The U.S. Court of Appeals for the Fourth Circuit considered a case factually similar to the instant case in *United States v. Simons*, 206 F.3d 392. The Foreign Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency ("CIA"), employed defendant Simons as an electrical engineer and provided him with an office and computer. *Id.* at 395. Similar to the DGS policy in the instant case, FBIS instituted a policy limiting Internet use by employees to official government business and prohibiting access to unlawful material. *Id.* at 395-96. The policy also stated that FBIS would "periodically audit, inspect, and/or monitor the

user's Internet access as deemed appropriate." *Id.* at 396. When FBIS obtained information indicating Internet traffic concerning sex through Simons' work computer, the agency remotely investigated Simons' Internet use and found visits to websites displaying images of nude women. *Id.* The agency then had the hard drive from Simons' work computer removed from his office, replaced with a copy, and produced the hard drive to an FBIS security officer, who turned it over to a criminal investigator with CIA Office of Inspector General ("OIG"). *Id.* After FBI special agents examined the hard drive and found files of child pornography, a federal search warrant was obtained to search Simons' office and computer. *Id.* at 396-97. Following indictment, Simons moved to suppress evidence from the searches, and the district court denied the motion. *Id.* at 397.

On appeal, the Fourth Circuit held that, in light of the FBIS Internet use policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet and that the retrieval of Simons' hard drive from his office did not violate his Fourth Amendment rights. *Id.* at 398-401. Addressing first the remote investigation of Simons' Internet use, the court determined that any subjective belief Simons had that his Internet use was private "was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use." *Id.* at 398. Similarly here, any subjective belief Defendant Cormack had in the digital contents of his work computer devices was not objectively reasonable in light of the DGS policy on Internet use and notice the Defendant regularly received that the use of his work computer was subject to monitoring, inspection, and disclosure at the discretion of authorized State personnel.

The *Simons* court separately addressed the warrantless entry into Simons' office. *Id.* at 399-401. Finding no evidence in the record of any workplace practices that would diminish

Simons' expectation of privacy, the court concluded that the entry into Simons' office constituted a Fourth Amendment search, but the search was reasonable and did not violate Simons' constitutional rights. *Id.*

In the instant case, however, Office C was regularly accessed by various DGS employees in order to obtain office supplies and other materials that were stored in the room, and the door was left open for that purpose during work hours. Indeed, Office C was "so open to fellow employees . . . that no expectation of privacy is reasonable." *O'Connor*, 480 U.S. at 718. The "operational realities" of Defendant Cormack's workplace "diminished his legitimate privacy expectations[,]" rendering any subjective privacy expectation he had in Office C objectively unreasonable. *Simons*, 206 F.3d at 399. During the entry to Office C on March 28, 2019, law enforcement did not invade or seize property from any potentially personal spaces (such as closed cabinets or drawers) and only seized State property. Therefore, neither the warrantless entry into Office C on March 28, 2019, nor the examination of his work computer and external hard drive was a Fourth Amendment search.

2. *United States v. Angevine*

In *United States v. Angevine*, another factually similar case, the Tenth Circuit held that no warrant was needed to examine a work computer seized from a university professor's office because warning banners displayed on the computer deprived the professor of any legitimate expectation of privacy. 281 F.3d at 1134-35. A police department obtained a warrant to search for child pornography on the defendant's work computer issued by the University employer and seized the computer from the defendant's office. *Id.* at 1132. Examination of the computer revealed that it was "used . . . to download over 3,000 pornographic images of young boys" that

were deleted after some were printed. *Id.* Notably, University officials "posted a 'splash screen' on University computers" that appeared "[e]ach time Professor Angevine turned on the computer in his office[.]" *Id.* at 1133. The warning banner stated, in part, that use of the computing system in any way contrary to law, University policies, and IT department policies was prohibited; that such prohibited use would make the user subject to disciplinary action and "may also subject [the user] to criminal penalties"; and that "[t]he University reserves the right to inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns of the University to the full extent not expressly prohibited by applicable statutes." *Id.* The defendant moved to suppress evidence from the search, arguing that material information was omitted from the warrant affidavit and requesting a *Franks* hearing. *Id.* at 1132. The district court denied on the motion on the grounds that a warrant was not required to conduct the search due to the defendant's lack of a legitimate expectation of privacy. *Id.*

On appeal, the Tenth Circuit affirmed the district court and determined that the University's "policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers." *Id.* at 1134. The court noted that the warning banner provided notice of potential criminal penalties, that the University reserved ownership of its computing system and the data stored in it, and that the defendant was issued the computer for work-related purposes only, making his relationship to the computer merely "incident to his employment." *Id.* at 1134-35. The court stated that it has "never held the Fourth Amendment protects employees who slip obscene computer data past network administrators in violation of a public employer's reasonable office policy." *Id.* at 1135.

The DGS computer use policy and warning banners in the instant case similarly put Defendant Cormack on notice that the State owned the computing system used by DGS employees and data stored on it, that the Defendant's work computer was to be used for authorized work-related purposes only, and that criminal penalties could attend unauthorized or unlawful use of the State's computing system. *See* Exhibit 2 (Acceptable Use Statement), Exhibit 3 (DGS Memorandum), Exhibit 5 (Warning Banners). The Defendant's relationship with his State-owned computer workstation was merely "incident to his employment" and not supportive of any privacy expectation. *Angevine*, 281 F.3d at 1135. To hold that investigators were not justified in entering Office C to examine the Defendant's work computer after a remote inspection proved inconclusive would give public employees constitutional cover to "slip obscene computer data past network administrators in violation of a public employer's reasonable office policy." *Id*. As the Angevine court recognized, the Fourth Amendment offers no protection to such violative uses of government-owned computing systems and therefore was not violated by the investigative measures taken at Office C on March 28, 2019.

3. *United State v. Bode*

In *United States v. Bode*, this Court considered whether the user of an Internet chat forum had a reasonable expectation of privacy in his chat messages where the website posted notices warning that messages were subject to logging and supervision and could be disclosed to authorities. Crim. No. ELH-12-158, 2013 WL 4501303, at *15–*20. The Court carefully considered applicable binding and non-binding case law, including the Fourth Circuit's decisions in *Simons* and *Hamilton* and the Tenth Circuit's decision in *Angevine*. *Id.* at *16-*20. The Court concluded that the website's "warning banners deprived Mr. Bode of any reasonable expectation

of privacy in his chat messages. As a result, [FBI agent's] review of Bode's logged messages did not constitute a search within the meaning of the Fourth Amendment." *Id.* at *20.

As in *Simons*, *Hamilton*, *Angevine*, and *Bode*, Defendant Cormack as a DGS employee had no reasonable expectation of privacy in his State-issued work computer or in his use of the State computing system. Like the computer use policy in *Simons*, the DGS computer use policy restricted use of the Defendant's work computer to lawful official and work-related purposes. *See* Exhibit 2 (Acceptable Use Statement), Exhibit 3 (DGS Memorandum). Like the policy in *Angevine*, the DGS policy prohibited unlawful use and materials and warned of disciplinary and criminal penalties. *Id.* In addition, the DGS policy prohibited access and storage of obscene and sexually explicit materials, like that eventually found in the Defendant's work computer. *Id.*

Furthermore, Defendant Cormack was on notice about the DGS policy and specifically warned on a frequent basis that he "should have no reasonable expectation of privacy" in the use of the State computing system. Exhibit 5 (Warning Banners). This warning was similar to the computer use policy at issue in *Hamilton*, which also expressly provided that users have "no expectation of privacy" in use of the computer system. *Hamilton*, 701 F.3d at 408. But, unlike *Hamilton*, there can be no question here as to whether Defendant Cormack was on notice of the policy. He encountered warning banners each time he logged into his work computer. These banners also provided that his use of the computer was subject to "monitoring, recording, copying, inspecting, and disclosure at the discretion of authorized personnel." Exhibit 5. By clicking "OK" upon receipt of this notice and proceeding with his log-in, the Defendant expressly consented to these terms. These warnings were, in substance, no less effective that those at issue in *Bode* and *Angevine* and provided more robust notice than the policies at issue in *Simons* and

Hamilton. Defendant Cormack cannot credibly or reasonably claim an expectation of privacy in the use of his work computer, so the investigation of his computer on March 28, 2019, was not a search under the Fourth Amendment. *See Davis*, 690 F.3d at 241 ("When there is no reasonable expectation of privacy, the Fourth Amendment is not implicated."). The Motion to Suppress should therefore be denied.

B. Any Search of Office C on March 28, 2019, Was Reasonable Under the Fourth Amendment.

Even if the Court determines that the entry into Office C and investigation of the Defendant's work computer on March 28, 2019, constituted a Fourth Amendment search, the search was reasonable under the Fourth Amendment. The Fourth Amendment only protects persons against "unreasonable" searches and seizures. *Simons*, 206 F.3d at 398 (quoting U.S. Const. amend. IV). "A search conducted without a warrant issued by a judge or magistrate upon a showing of probable cause is '*per se* unreasonable' unless it falls within one of the 'specifically established and well-delineated exceptions' to the warrant requirement." *Id.* at 399–400 (citation omitted). These well-established exceptions include searches conducted by consent and workplace searches. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) ("one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent"); *O'Connor*, 480 U.S. at 725-26 ("public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances"). Here, valid consent was provided by both an authorized State official and the Defendant himself, and, even

without consent, the workplace search would have been reasonable both in its inception and in its scope under *O'Connor*.

1. Any Search that Occurred on March 28, 2019, Was a Reasonable Search by Consent.

Valid consent is a well-established exception to the warrant requirement. *United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973)). The Government must show valid consent to search by a preponderance of the evidence. *Id*. "Consent to search is valid if it is (1) 'knowing and voluntary,' . . . and (2) given by one with authority to consent[.]" *Id.* (citations omitted). Voluntary consent can be provided by the defendant or by "a third party who possessed common authority over . . . the premises." *United States v. Shrader*, 675 F.3d 300, 306 (4th Cir. 2012) (quoting *United States v. Matlock*, 415 U.S. 164, 171 (1974)). Consent may be express or implied; it "may be inferred from actions as well as words." *Hylton*, 349 F.3d at 786.

The voluntariness of consent is "a question of fact to be determined from the totality of all the circumstances." *Schneckloth*, 412 U.S. at 227, *quoted in United States v. Azua-Rinconada*, 914 F.3d 319, 324 (4th Cir. 2019). In *Schneckloth*, the Supreme Court emphasized key distinctions between a waiver of Fourth Amendment rights by consenting to a search and a waiver of constitutional protections of a defendant's rights at trial. 412 U.S. 218, 242–43. "[U]nlike those constitutional guarantees that protect a defendant at trial, it cannot be said every reasonable presumption ought to be indulged against voluntary relinquishment." *Id.* at 243. Valid consent does not render a search "somehow 'unfair[,]'" and "there is nothing constitutionally suspect in a person's voluntarily allowing a search." *Id.* at 242-43.

Here, consent to the March 28, 2019, investigation was provided both by the Defendant and by State officials with authority over the matter searched.

a. Defendant Consented to Any Search of State Computer Equipment.

The Defendant consented to monitoring of his use of his State-issued work computer and to disclosure of that information to authorities each time he logged into the computing system at work. *See* Exhibit 5 (warning banner stating in part, "Anyone using this system ***expressly consents*** to such monitoring, recording, copying, inspecting, and disclosure at the discretion of authorized personnel.") (emphasis added).

As an alternative basis for denying the suppression motion in *Bode*, this Court held that defendant Bode consented to the examination of his private chat messages by law enforcement. *Bode*, 2013 WL 4501303, at *20. One of the warning banners used on the website at issue stated in part that "[a]ll posted pictures and conversations, public and private, are logged and supervised[,]" and that the website could "disclose these communications to the authorities at its discretion." *Id.* Additionally, "on each occasion that Bode logged in, he was required to click a button labeled 'ACCEPT' immediately below the stated terms." *Id.* Thus, even if the FBI special agent's examination of Bode's chat messages was a Fourth Amendment search (which this Court determined it was not), Bode's acceptance of the website's terms "was sufficient to constitute his consent to the search." *Id.*; *see also Linder*, 2012 WL 3264924, at *12 ("[P]er DOJ and USMS policies Linder consented to the search of his computer and Blackberry by using them."). Any "search" of the chat messages, therefore, was reasonable under the Fourth Amendment.

In the instant case, Defendant Cormack voluntarily affirmed his consent to monitoring, recording, and disclosure of his computer use each time he logged in by clicking "OK" under a warning banner. *See* Exhibit 5. His consent justified any search of his work computer as reasonable.

In *Bode*, this Court rejected defendant Bode's argument that the FBI's review of his messages exceeded the scope of his consent, noting the provision in the warning banner that logged messages could be disclosed to authorities. 2013 WL 4501303, at *20. Notably, the Court found "no meaningful distinction between giving a copy of the log to [the FBI special agent], on the one hand, and giving [the special agent] access to view the copy of the log stored on [the website's] servers, on the other hand." *Id.*

Similarly here, one of the warning banners Defendant Cormack encountered when logging in expressly stated that his use of the computer system constituted consent to "disclosure at the discretion of authorized personnel." Exhibit 5. Members of Maryland Capital Police, as the security component of DGS, and DoIT, as the department charged with managing DGS's computer system, are "authorized personnel" that enjoyed the discretion of making disclosures to MSP about the Defendant's work computer use. In addition, DGS's policy on employee computer use, which the Defendant acknowledged receiving, warns of both disciplinary actions and "civil or criminal prosecution" for violations of the policy. Exhibit 2 (Acceptable Use Statement). Thus, the Defendant consented to disclosure concerning his work computer use for the purpose of a criminal investigation. That law enforcement participated in the examination of the Defendant's work computer on March 28, 2019, was not outside the scope of his consent. Indeed, "there is no meaningful distinction between" MSP being provided copies of the Defendant's work hard drives,

on the one hand, and MSP directly obtaining these computer images at the State facility with the consent of DoIT and Maryland Capitol Police, on the other hand. *Bode*, 2013 WL 4501303, at *20.

The Defendant's consent justified and rendered reasonable any Fourth Amendment search that occurred on March 28, 2019. The Motion to Suppress should be denied.

b. Authorized State Officials Consented to Any Search of State Computer Equipment.

Proof of voluntary consent is "not limited to proof that consent was given by the defendant[.]" *United States v. Matlock*, 415 U.S. 164, 171 (1974). It may be satisfied by permission "obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *Id*. "[T]he consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared." *Id.* at 170. In sharing use of the property, the nonconsenting person shares authority over it and assumes the risk that another user might permit the property to be searched. *Buckner*, 473 F.3d at 554 (citing *Matlock*, 415 U.S. at 171).

Valid consent can be provided by a person with either actual authority or apparent authority to consent to the search. *Id.* at 555 (citing *Illinois v. Rodriguez*, 497 U.S. 177, 188 (1990)). Apparent authority exists when the facts available to the government at the time of consent support "an objectively reasonable belief" that the consenting party had authority to consent to the search. *Id.*; *see also Rodriguez*, 497 U.S. at 188. Whether the person providing consent had authority to do so "depends on viewing these facts in light of the *totality* of the circumstances known to the officers at the time of the search." *Buckner*, 473 F.3d at 555. "The determination of consent to

enter must be judged against an objective standard, whether the facts available to the officer warrant a man of reasonable caution in the belief that the consenting party had authority over the premises." *United States v. Preston*, 9 F.3d 1545 (4th Cir. 1993) (unpublished) (citing *Rodriguez,* 497 U.S. at 188).

An employer may consent to a Fourth Amendment search of a workplace and facilities the employer controls.

> [C]ourts have long recognized that employers, as third parties who possess common authority over the workplace, may independently consent to a search of an employee's workplace documents or communications. This rule is a logical application, in the workplace context, of general principles governing third-party consent. An individual or entity exercising common authority over the place or thing to be searched may independently consent to a search.

Walker v. Coffey, 905 F.3d 138, 148-49 (3d Cir. 2018) (citing *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968), and *Matlock*, 415 U.S. at 171) (footnotes omitted). In *Walker*, the Third Circuit held that emails Walker sent and received via "an email system controlled and operated by Penn State[,]" Walker's employer, "were subject to the common authority of [the employer]." *Id.* at 149. "Walker did not enjoy any reasonable expectation of privacy vis-à-vis Penn State, and Penn State ***could independently consent*** to a search of Walker's work emails." *Id.* (emphasis added).

Likewise, "[c]ourts have . . . concluded that an employer having administrative access to an employee's computer could validly consent to a search of the computer, even when the computer is password-protected and contains non-work-related, personal files of the employee." *United States v. Waddell*, No. 18-10980, 2020 WL 7647515, at *6 (11th Cir. Dec. 23, 2020) (unpub.) (citing *United States v. Ziegler*, 474 F.3d 1184, 1192 (9th Cir. 2007)); *see also Linder*, 2012 WL 3264924, at *12 ("[B]ecause the Blackberry and computer files were within the control

of Linder's employer, his employer can give consent to search them."); *United States v. England*, No. 6:18-CR-56-CHB-HAI, 2019 WL 9633210, at *4 (E.D. Ky. Dec. 11, 2019), *report and recommendation adopted,* No. 6:18-CR-056-CHB, 2020 WL 2110801 (E.D. Ky. May 4, 2020) (finding that fire chief had "common authority over or other sufficient relationship to" city-owned laptop that he issued to fire lieutenant and therefore had actual and apparent authority to consent to search of laptop because "the culture, customs, and expectations in the fire department were such that [fire chief] was ultimately in charge of the laptop and could obtain or use it at any time[,]" and "members of the fire department 'assumed the risk' that [fire chief could permit the laptops to be searched") (quoting *Matlock*, 415 U.S. at 171).

In *United States v. Ziegler*, the Ninth Circuit held that a private employer could consent to a government search of an employee's office and the computer it provided the employee to work. 474 F.3d 1184, 1192 (9th Cir. 2007). The court noted that "employees were apprised of the company's [computer] monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature." *Id.* In considering whether the employer exercised common authority over the employee's office, the court examined the Supreme Court's decision in *Mancusi* and determined that, "even where a private employee retains an expectation that his private office will not be the subject of an unreasonable government search, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns." *Id.* at 1191.

In the instant case, DGS and DoIT, both departments of the State of Maryland, enjoyed control and ownership of Office C and DGS's computing system as a whole and therefore common authority to consent to searches of both State facilities. DGS's policy on computer use and the

warning banners DoIT displayed during the log-in process of DGS work computers made explicit that employees did not enjoy a reasonable expectation of privacy vis-à-vis the State of Maryland and that the State asserted control and ownership of its facilities and specifically its computing system. *See* Exhibit 2 (Acceptable Use Statement), Exhibit 3 (DGS Memorandum), Exhibit 5 (Warning Banners). With regular notice of these policies and warnings, Defendant Cormack assumed the risk that his employer would permit law enforcement access to his work computer.

Officials of both DoIT and Maryland Capitol Police, a component of DGS, were personally involved in the entry to Office C and the examination of the Defendant's work computer on March 28, 2019, and, both by words and by deeds, they consented to these investigative steps.

Specifically, the Chief Information Security Officer of DoIT signed a written authorization for MSP to search, seize, and examine images of the Defendant's State-owned computer and external hard drive from Office C. Exhibit 6 (Consent). This State official had both actual and apparent authority to provide consent. DoIT is responsible for the administration of the computer systems utilized by DGS in the performance of its functions. One of the warning banners DGS employees encounter when logging into their work computers states at the outset, "This computing system is owned and operated by the State of Maryland, Department of Information Technology, and is for official use only by authorized personnel." Exhibit 5. Additionally, DoIT's logo is displayed prominently on the warning banners. *See id.* As the owner and operator of the computer system utilized by DGS that, according to the warning banners, has reserved to itself the authority to monitor, record, copy, inspect, and disclose any files stored in the computer system and any information about the use of the system, *see id.*, DoIT had both actual and apparent authority to consent to any Fourth Amendment search and seizure regarding the computer system.

With the consent of the Chief Information Security Officer, any such search and seizure was reasonable under the Fourth Amendment.

As the security component of DGS, the agency that controlled Office C, Maryland Capitol Police also had authority to access Office C and to consent to such access. *See United States v. Kirby*, No. 3:15-CR-175-J-32JBT, 2016 WL 11677006, at *9–*10 (M.D. Fla. July 7, 2016), *report and recommendation adopted,* No. 3:15-CR-175-J-32JBT, 2016 WL 11677005 (M.D. Fla. Aug. 2, 2016) (Live Oak Police Department ("LOPD"), as a department of the City of Live Oak, had actual and apparent authority to search City-owned computers, and "to consent to their search and seizure by the FBI," in light of "the policies, procedures, and office practices of the City and the LOPD," which deprived defendant of any reasonable expectation of privacy in the computers).

Any Fourth Amendment search of Office C and the Defendant's work computer conducted with valid consent and therefore reasonable. The Motion to Suppress should be denied.

2. Any Search that Occurred on March 28, 2019, Was a Reasonable Government Workplace Search.

The Supreme Court has long recognized that a government employer has special needs to enter spaces that may be protected by the Fourth Amendment but outweigh any countervailing privacy interests and may therefore justify warrantless entry and search. These needs include "the government's need for supervision, control, and the efficient operation of the workplace[,]" *O'Connor*, 480 U.S. 709, 719–20, and the need to investigate "work-related employee misconduct[,]" *id.* at 724. "[W]hen a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope." *Simons*, 206 F.3d at 400 (citing *O'Connor,* 480 U.S. at

725-26). In this situation, "a warrant or probable cause standard does not apply. . . ." *Gossmeyer v. McDonald*, 128 F.3d 481, 490 (7th Cir. 1997) (citing *O'Connor*, 480 U.S. at 719–26). A government workplace search is "justified at its inception" when "there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct[.]" *O'Connor*, 480 U.S. at 726. A workplace search is "permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct." *Id.* (internal quotation marks and brackets omitted). It is important to note, however, that a reasonable Fourth Amendment search need not be "the 'least intrusive' search practicable[.]" *Quon*, 560 U.S. at 763.

In *Simons*, the Fourth Circuit recognized that, even where "the *dominant purposes* of the warrantless search of [an employee's] office was to acquire evidence of criminal activity," "the search remains within the *O'Connor* exception to the warrant requirement[,]" provided that the criminal activity was committed at the workplace using the employer's facilities. 206 F.3d at 400 (emphasis added); *see also Linder*, 2012 WL 3264924, at *11 ("A workplace search still falls within the *O'Connor* framework even if the purpose of the search is to discover evidence of criminal activity."). In this situation, the employer "did not lose its special need for 'the efficient and proper operation of the workplace,' . . . merely because the evidence obtained was evidence of a crime." *Simons*, 206 F.3d at 400 (citing *O'Connor,* 480 U.S. at 723). Thus, the fact that FBIS did not utilize the hard drive seized from defendant Simons' office "for internal investigatory purposes before turning it over to the criminal investigator at OIG" did not render law enforcement's warrantless examination of the hard drive unreasonable under the Fourth Amendment. *Id.*; *see also Gossmeyer*, 128 F.3d at 492 ("Case law . . . instructs that the presence

of outside law enforcement officials and the possibility of the search leading to criminal charges against Gossmeyer did not inevitably convert the search into a criminal search requiring probable cause and a warrant.").

In the instant case, any search that occurred on March 28, 2019, at Office C was both reasonable in its inception and in scope and therefore reasonable under the Fourth Amendment.

The search was "justified at its inception" because the credible report of Witness 1 that Defendant Cormack viewed an image of child sexual abuse on his work computer gave DGS and DoIT "reasonable grounds for suspecting" that examination of the work computer and related storage media would turn up evidence of work-related misconduct by the Defendant. *O'Connor*, 480 U.S. 709, 726 (1987); *see also Gossmeyer*, 128 F.3d at 491 (search of Gossmeyer's cabinets was "justified at its inception" where anonymous co-worker "made serious and specific allegations of misconduct—that Gossmeyer had pornographic pictures of children; and stated where those pictures could be found—in Gossmeyer's file cabinets and desk"). Witness 1's statements to Maryland Capitol Police, the security component of DGS, exhibited many signs of reliability, including

- statements that he has known Defendant Cormack for many years, was familiar with the Defendant's family;
- detailed description of the image he saw in January 2019 on the Defendant's computer and how the Defendant responded to Witness 1's presence (immediately closing the screen displaying the image);
- details about instances in which the Defendant exhibited similar behavior over the years;
- detailed description, with a hand drawing, of the Defendant's workspace and the position of his work computer and personal computer; and

- statements that reporting what he saw to authorities was difficult for him (given his long-standing relationship with the Defendant) but that he felt it was the right thing to do.

Importantly, Witness 1's report provided indication of unauthorized and unlawful use of the State's computing system by Defendant Cormack, in violation of DGS's policy against using State-owned computers to access or store sexual and obscene material. *See* Exhibit 2 (Acceptable Use Statement), Exhibit 3 (DGS Memorandum).

Based upon this report of work-related misconduct and potentially criminal activity, DoIT undertook a remote examination of Defendant Cormack's computer use, which was well within the scope of its authority to monitor and inspect use of the State computing system. *See* Exhibit 5 (Warning Banners). The Chief Information Security Officer ultimately determined that he could not obtain the Defendant's Internet search history.

The State officials and criminal investigators involved in the investigation then determined to conduct a direct examination of the Defendant's work computer located in Office C. Entry into Office C was necessary to further the investigation of Defendant Cormack's misconduct. Once entry was made, the investigators' activities were focused on examining information stored in the Defendant's State-issued computer and external hard drive. These measures were "reasonably related to the objectives" of entry into Office C, "not excessively intrusive in light of the nature of the misconduct[,]" and therefore "permissible in . . . scope[.]" *O'Connor*, 480 U.S. at 726 (internal quotation marks and brackets omitted).[1] It was also reasonable to conduct the

1 To the extent that the investigator's activities in Office C exceeded examination and imaging of State-issued computer equipment, it is immaterial because the only information gained from the investigation on March 28, 2019, that contributed to subsequent search warrants was derived from the forensic preview

investigation after work hours in order to avoid alerting the Defendant to the investigation, which might prompt him to destroy evidence and undermine the integrity of the investigation.

As the Fourth Circuit recognized in *Simons*, even if the "dominant" purpose of the foregoing investigative measures "was to acquire evidence of criminal activity[,]" the Defendant's employer still had a special need to investigate his work-related misconduct and to protect the State's computing system from unauthorized and unlawful uses. 206 F.3d at 400. Therefore, the investigation at Office C on March 28, 2019, was a reasonable workplace search under *O'Connor*, in addition to being justified by consent, and therefore did not violate the Defendant's Fourth Amendment rights. The Motion to Suppress should be denied.

C. Any Search of Office C on March 28, 2019, Was Justified by Good-Faith Reliance on Binding Circuit Precedent.

As the Supreme Court has held, "Suppression of evidence has always been our last resort, not our first impulse." *Utah v. Strieff*, 136 S. Ct. 2056, 2061 (2016). In *Davis v. United States*, the Supreme Court recognized the "heavy toll on both the judicial system and society at large" exacted by the exclusion of "reliable, trustworthy evidence bearing on guilt or innocence." 564 U.S. 229, 237 (2011) (citation omitted). The "bottom-line effect" of the exclusionary rule in many cases, such as the instant case, would be "to suppress the truth and set the criminal loose in the community without punishment." *Id.* The purpose of the exclusionary rule is to deter patterns of unconstitutional police action, but "isolated, nonrecurring police negligence . . . lacks

---

of the computer and external hard drive and subsequent examination of these State-issued devices. This scope of these activities was reasonable.

the culpability required to justify the harsh sanction of exclusion." *Id.* at 239 (citing *Herring v. United States*, 555 U.S. 135, 137 (2009)) (internal quotation marks and brackets omitted).

Thus, "even if a search is judged to be constitutionally flawed in some way, its fruits need not be suppressed if the agents acted 'in reasonable reliance on binding precedent.'" *United States v. Kolsuz*, 890 F.3d 133, 147 (4th Cir. 2018) (quoting *Davis*, 564 U.S. at 241). "In such circumstances, suppression can do little to deter police misconduct, and the 'social costs' of suppression—the exclusion from trial of reliable evidence bearing on guilt or innocence—outweigh any deterrence benefits." *Id.* (citing *Davis*, 564 U.S. at 237–38).

Under *Davis*, even if this Court finds that the investigation of Defendant Cormack's work computer at Office C was an unconstitutional search, the fruits of the search should not be suppressed because the investigators acted "in reasonable reliance on binding precedent." *Davis*, 564 U.S. at 241. Binding case law in the Fourth Circuit held that government employees lack any legitimate expectation of privacy in their use of work computing systems when they are on notice that such computer use is subject to monitoring and that the employee should not expect privacy in their computer use. *See Simons*, 206 F.3d at 398. Binding precedent in the Fourth Circuit also held that warrantless entry into a government employee's office in order to investigate work-related misconduct in computer use was reasonable under the Fourth Amendment. *See id.* Under *Simons*, such investigative measures are no less reasonable even when undertaken for the "dominant" purpose of a criminal investigation. *Id.*

Here, the investigators who entered Office C on March 28, 2019, to investigate Defendant Cormack's unauthorized and unlawful activity on his work computer reasonably relied upon

Simons as binding precedent in the Fourth Circuit. Therefore, the fruits of their efforts should not be subjected to the harsh sanction of exclusion, and the Court should deny the Motion to Suppress.

D. Each of the Challenged Search Warrants Was Supported by Probable Cause.

The Motion to Suppress challenges searches of Defendant Cormack's residence and Office C that occurred on May 2, 2018, pursuant to state search warrants, and the forensic examination of devices seized from those locations pursuant to a federal search warrant. The Court should reject this challenge because each search warrant was well-supported by an affidavit confirming probable cause to believe that evidence of child pornography offenses would be found in each location.

When law enforcement undertakes a search for evidence of criminal activity, the Fourth Amendment generally requires a judicial warrant supported by probable cause. *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). To determine whether there was probable cause to support a search warrant, the courts apply the totality-of-the-circumstances test set forth in *Illinois v. Gates*, 462 U.S. 213, 233 (1983). As the Supreme Court stated,

> [t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a "substantial basis for . . . conclud[ing]" that probable cause existed.

Id. at 238 (citation omitted). The Court further stated that "the term 'probable cause,' according to its usual acceptation, means less than evidence which would justify condemnation. . . . It imports a seizure made under circumstances which warrant suspicion." *Id.* at 235 (citation omitted).

"Finely-tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision. . . . [I]t is clear that 'only the probability, and not a prima facie showing, of criminal activity is the standard for probable cause.'" *Id.* (citations omitted). "[T]he nexus between the place to be searched and the items to be seized may be established by the nature of the item and the normal inferences of where one would likely keep such evidence." *United States v. Richardson*, 607 F.3d 357, 371 (4th Cir. 2010) (quoting *United States v. Anderson*, 851 F.2d 727, 729 (4th Cir.1988)).

A reviewing court is to show great deference to the magistrate's conclusion in considering whether the magistrate had a substantial basis for finding probable cause. *Id.* at 236. "[C]ourts should not invalidate warrants by interpreting affidavits in a hypertechnical, rather than a common-sense manner." *Id.*; *see also United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

Each of the three search warrants challenged in the Motion sought authorization to seize evidence of child pornography offenses, and each was well-supported by probable cause to believe that the location to be searched would reveal such evidence.

The affidavit in support of the state warrants to search Office C and the Defendant's residence at 24 Lyndale Avenue, Nottingham, Maryland were signed by TFC Frank Donald of MSP. *See* Exhibit 7 (Search Warrant for Office C), Exhibit 8 (Search Warrant for Residence). The warrants were signed by the Honorable Wayne A. Brooks of the District Court of Howard County, Maryland on April 29, 2019. *See id.*

The affidavit in support of the federal warrant to examine devices seized from the Defendant was signed by HSI Special Agent Augustus Aquino. *See* Exhibit 9 (Search Warrant

for Devices). The federal search warrant was signed by the Honorable J. Mark Coulson, U.S. Magistrate Judge of the U.S. District Court for the District of Maryland. *See id.*

Each of the three affidavits stated, in substance and in part, the following:

a. An employee of DGS ("Anonymous" or "Witness 1") observed what he believed to be child pornography on a co-worker's computer screen.

b. On February 5, 2019, TFO Donald of MSP and Sergeant Warren Smith of Maryland Capitol Police met with Witness 1, and Witness 1 stated the following, in part:

- Witness 1 went into Defendant Cormack's workspace and saw an image of what he believed to be child pornography on the Defendant's State computer. The image depicted a male child of approximately 8 years of age posing in white underwear who appeared to be terrified. Witness 1 was certain that the intended purpose of the image was for sexual gratification. The Defendant immediately minimized the image file when Witness 1 walked into the room.

- A similar incident occurred several years prior when Witness 1 observed the Defendant viewing a suspicious website on his personal computer and observed the title "young Japanese boys" on the site. Witness 1 regretted not reporting the prior incident but that he had considered it a fluke. Witness 1 noticed several "red flag" instances over the years, and the Defendant's behavior had continued without stopping.

- Defendant Cormack was charged for several sexual offenses in approximately 1995.

- Defendant Cormack was "very into computers," tended to migrate from his work computer to his personal computer during the work day, and had a back-up drive that went home with him every night. The Defendant kept his personal laptop computer in the back of Office C near the supplies closet and, whenever someone approached, the Defendant closed the display. The Defendant always took his personal laptop with him to and from work.

- It pained Witness 1 to report Defendant Cormack. Witness 1 was certain of what he saw and felt that an investigation was warranted.

c. Witness 1 provided a hand-drawn map of Office C that depicted the location of Defendant Cormack's work and personal computer.

d. TFO Donald contacted the Baltimore County Police Department and obtained a copy of the report from 1996 investigation of Defendant Cormack. The investigation concluded that Defendant Cormack sexually abused several boys while employed as a Baltimore County Recreation Counselor between 1979 and 1984.

e. On March 28, 2019, TFO Donald and members of the MSP Digital Forensics Lab, DoIT, and Maryland Capitol Police entered Office C after work hours. DoIT provided MSP with consent to search and seize Defendant Cormack's work computer and external hard drive.

f. During a preview of the hard drive, TFO Donald observed an image of a male believed to be 14 to 15 years old masturbating his erect penis. All items in Cormack's office area were photographed and replaced in their original place as to not cause any suspicion of the active investigation.

g. The work computer hard drive was cloned, and the external hard drive that was connected to the work computer was imaged. There were cables attached to Defendant Cormack's work computer that would allow him to easily attach an external hard drive, but there were no external hard drives attached to said cables.

h. On April 18, 2019, members of MSP, including a digital forensic examiner, reviewed Defendant Cormack's work computer hard drive and external hard drive. The officers found, in part, the following:

- on March 8, 2018, the work computer was used to search the internet for "child porn" on 12 separate occasions;
- on September 28, 2018, a search was conducted on Youtube for "boys skinny dipping";
- several images of scantily clothed and shirtless prepubescent males;
- information about child sexual abuse material, illegal images, and child pornography crimes was visited; and
- Defendant Cormack's work computer referenced that an additional external hard drive was frequently connected.

i. An MVA query of Defendant Cormack revealed that he used the address of 24 Lyndale Avenue, Nottingham, Maryland. On April 26, 2019, TFO Donald conducted visual surveillance of the address and observed, at 6:30 a.m., an elderly Caucasian male exit the house carrying a travel bag and enter a vehicle registered to Defendant Cormack.

Each of the three affidavits also provided general information about computer-related investigations of child exploitation offenses and common characteristics of persons involved in possessing and collecting child pornography, including common practices of obtaining child pornography through use of computers, long-term electronic storage of this material, and the storage of computers and other electronic media in residences and places hidden from view.

In addition, Special Agent Aquino's affidavit in support of the federal search warrant to examine seized storage media stated the following:

a. On May 2, 2019, MSP executed the state search warrants with the assistance of HSI and seized numerous digital devices listed in Attachment A.

b. Defendant Cormack waived Miranda rights, agreed to be interviewed, and stated the following, in part:

- The briefcase Defendant Cormack ordinarily takes to work with him was located in his car, which was parked in front of his house. The briefcase contained two external hard drives, and one of the hard drives contained a back-up of the files in which the Defendant archives for work. Defendant Cormack backs up the files out of caution since files contained on the office network server have been lost in the past. The other hard drive contains photos of family and vacations and personal documents. There was no "pornography" on this hard drive.

- The Defendant did not use his work computer to view child pornography but he had used Google and, if child pornography came up, he would look at it.

- Defendant Cormack had a personal laptop computer at work that should be located in his office, either on the desk or in a grey cabinet. It was an Acer laptop computer, and he usually does not bring it home. The Defendant has the personal laptop at his work site because he has a color printer he uses to print out pictures of family and vacations to display in his office.

- Defendant Cormack did not produce, distribute, or save any child pornography, but he had looked at child pornography. The Defendant went on "Google at work" to look at child pornography and did not remember any search terms or used any specific "sites."

The foregoing facts, and others outlined in the search warrants affidavits, provided ample probable cause to believe that Office C and the Defendant's residence would contain the evidence sought, including storage media that would, in turn, contain evidence of child pornography offenses. The affidavits also detailed a nexus between the child pornography crimes under investigation and each of the locations to be searched.

The nexus to Office C was detailed in the warrant affidavit, in part, by the following:

- A reliable and detailed account from a co-worker of the Defendant ("Witness 1") who knew the Defendant for several years and was an eyewitness to the Defendant recently viewing in image of child sexual abuse on his work computer in Office C and similar incidents in the past;[2]

- Witness 1's statements that the Defendant commonly possessed a personal computer in Office C and that the Defendant commonly used both his work computer and personal computer during the work day, as well as detailed description of where the Defendant's personal computer was typically located in Office C;

- The consent seizure of the Defendant's State-issued external hard drive and State-issued work computer from Office C;

- The forensic preview of the external hard drive and the subsequent examination of the work computer, which revealed child pornography and Internet searches indicative of an interest in child pornography and sexual interest in children;

- Evidence that the Defendant's work computer had frequently connected to another external hard drive that was not connected at the time the work computer's hard drive was seized.

2 As described above, Witness 1's statements exhibited many signs of reliability, including his long-term familiarity with the Defendant and how his work and personal computers were kept in Office C, the detailed character of his report, and statements that reporting what he saw to authorities was difficult for him but that he felt it was the right thing to do.

The nexus to 24 Lyndale Avenue, Nottingham, Maryland was detailed in the warrant affidavit, in part, by the following:

- Witness 1's statements about the Defendant transporting electronic storage devices between work and home;
- Evidence that the Defendant's work computer had frequently connected to another external hard drive that was not connected at the time the work computer's hard drive was seized;
- MVA records indicating that 24 Lyndale Avenue, Nottingham, Maryland was the Defendant's residence;
- The observation of TFC Donald that an individual matching the Defendant's description carried a travel bag from the residence to a vehicle registered to the Defendant in the morning, before work hours;
- The common practice of child pornography offenders to keep their collections of child pornography in their residences, including in computers and other storage media.

The nexus to the electronic storage devices seized from Office C and the Defendant's residence was supported in Special Agent Aquino's affidavit by all of the foregoing and the following:

- Defendant Cormack's statement, following denials, that he viewed child pornography through Google, a website accessed through use of a computer;
- The Defendant's statement that he kept a personal computer at work, in Office C.

In summary, each of the search warrants was supported by probable cause. Therefore, evidence obtained from the searches of Office C, the Defendant's residence, and the seized storage media should not be suppressed. The Motion to Suppress should be denied.

E. Searches Pursuant to the Warrants Were Justified by Good Faith.

Even if the Court determines that the showing of probable cause in any of the search warrant affidavits was not sufficient, the seized evidence and any derivative evidence remain admissible pursuant to the good faith exception enunciated in *United States v. Leon*, 468 U.S. 897 (1984). Under *Leon*, "a court should not suppress the fruits of a search conducted under the authority of a warrant, even a 'subsequently invalidated' warrant, unless 'a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Bynum*, 293 F.3d 192, 195 (4th Cir. 2002) (quoting *Leon,* 468 U.S. at 922 n.23). The good faith exception applies "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Leon*, 468 U.S. at 920; *see also United States v. Perez*, 393 F.3d 457 (4th Cir. 2004) (reversing district court's decision granting motion to suppress and finding that good faith exception cured the problems raised regarding the search warrant).

Here, TFO Donald and Special Aquino acted with objective good faith in obtaining warrants to search Office C, the Defendant's Residence, and storage media seized from those locations, and law enforcement acted within the scope of each warrant in executing it. There was no facial defect in any of the warrants. Thus, even if the Court finds any of the warrants invalid, evidence obtained from the searches should not be suppressed under the good faith exception in *Leon*. The Motion to Suppress should be denied.

III. CONCLUSION

For all of the above reasons, the government respectfully requests that the Court deny the Motion to Suppress.

Respectfully submitted,

Jonathan F. Lenzner
Acting United States Attorney

/s/
By: _____
Matthew J. Maddox
Assistant United States Attorney

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on this 20th day of March, 2021, a copy of the foregoing Government's Response in Opposition to Defendant's Motion to Suppress Tangible and Derivative Evidence was electronically filed with notice to counsel of record.

By: /s/
Matthew J. Maddox
Assistant United States Attorney